PRUEBA DE HABILIDADES PRACTICAS CCNA

ZARINA ESTHER GONZALEZ PAEZ

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA "UNAD"

ESCUELA DE CIENCIAS BASICAS Y TECNOLOGIAS

INGENIERIA DE SISTEMAS

CEAD VALLEDUPAR

2019

PRUEBA DE HABILIDADES PRÁCTICAS CCNA

ZARINA ESTHER GONZALEZ PAEZ

DIPLOMADO DE PROFUNDIZACIÓN CISCO (DISEÑO E IMPLEMENTACIÓN DE SOLUCIONES INTEGRADAS LAN / WAN)

GRUPO 203092_19

TUTOR
GIOVANNI ALBERTO BRACHO

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA "UNAD"
ESCUELA DE CIENCIAS BASICAS Y TECNOLOGIAS
INGENIERIA DE SISTEMAS
CEAD VALLEDUPAR
2019

TABLA DE CONTENIDO

INTRODUCCION

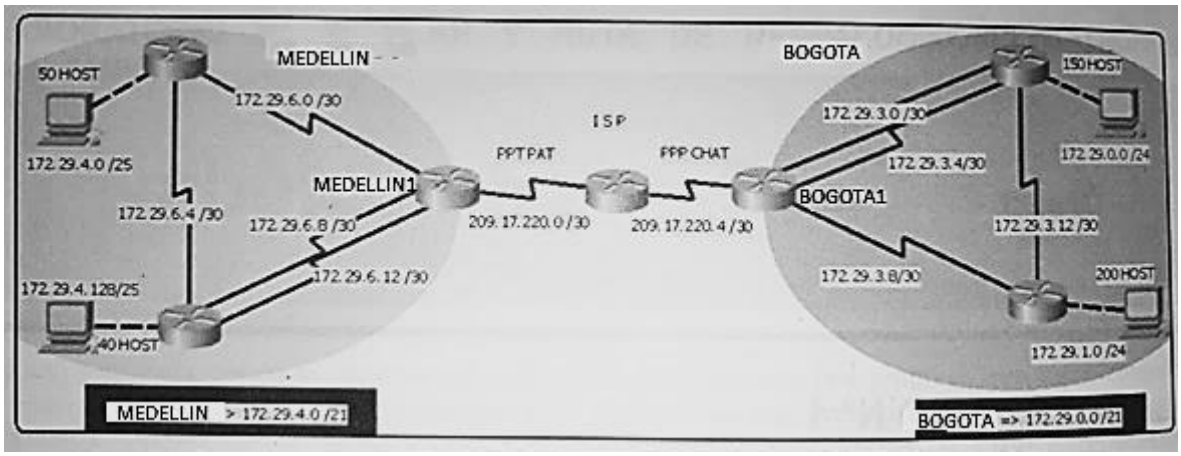
En el siguiente trabajo consiste en implementar todo el conocimiento adquirido durante el Diplomado de profundización CISCO, diseño e implementación de soluciones integradas LAN / WLAN, los cuales fueron puestos en práctica con dos ejercicios.

Las Redes informáticas son un mecanismo que ha hecho que la vida moderna cambie totalmente, con el uso del Internet la vida del ser humano ha cambiado tanto que ahora todo es mas veloz y fácil, es hay donde nos damos cuenta la importancia que tienen las redes a nivel mundial.

El desarrollo de los ejercicios fue realizado en Packet Tracer con el cual hemos venido trabajando a lo largo del curso con el fin de demostrar las habilidades adquiridas.

1.0 DESCRIPCION DEL ESCENARIO 1

Una empresa posee sucursales distribuidas en las ciudades de Bogotá y Medellín, en donde el estudiante será el administrador de la red, el cual deberá configurar e interconectar entre sí cada uno de los dispositivos que forman parte del escenario, acorde con los lineamientos establecidos para el direccionamiento IP, protocolos de enrutamiento y demás aspectos que forman parte de la topología de red.



Este escenario plantea el uso de RIP como protocolo de enrutamiento, considerando que se tendrán rutas por defecto redistribuidas; asimismo, habilitar el encapsulamiento PPP y su autenticación.

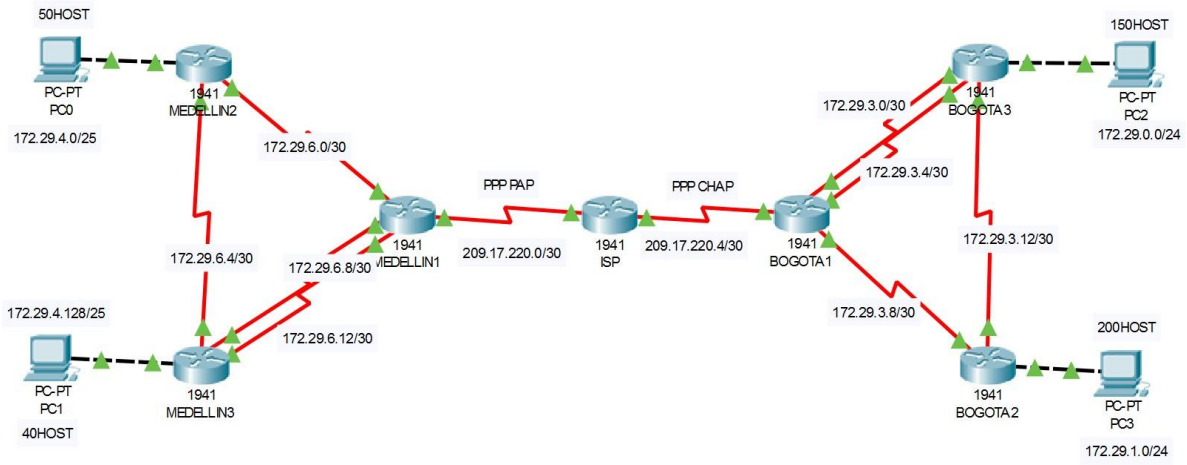
Los routers Bogota2 y medellin2 proporcionan el servicio DHCP a su propia red LAN y a los routers 3 de cada ciudad.

Debe configurar PPP en los enlaces hacia el ISP, con autenticación.

Debe habilitar NAT de sobrecarga en los routers Bogota1 y medellin1.

1.1 SOLUCION DEL ESCENARIO 1

1.1.1 Topología



1.1.2 CONFIGURACIÓN BÁSICA DE DISPOSITIVOS

Configuración Básica ISP

Hostname: **ISP**

Enable secret: **itsaseret**

Password Line Console 0: **cisco**

Password Line vty 0 15: **cisco**

Service password-encryption

Banner motd “Acceso solo al personal autorizado”

Configuración Básica MEDELLIN1

Hostname MEDELLIN

Enable secret: **itsasecret**

Password Line Console 0: **cisco**

Password Line vty 0 15: **cisco**

Service password-encryption

Banner motd “Acceso solo al personal autorizado”

Configuración Básica BOGOTA1

Hostname BOGOTA

Enable secret: **itsasecret**

Password Line Console 0: **cisco**

Password Line vty 0 15: **cisco**

Service password-encryption

Banner motd “Acceso solo al personal autorizado”

Configuración Básica BOGOTA2

Hostname BOGOTA2

Enable secret: **itsasecret**

Password Line Console 0: **cisco**

Password Line vty 0 15: **cisco**

Service password-encryption

Banner motd “Acceso solo al personal autorizado”

Configuración Básica BOGOTA3

Hostname BOGOTA3

Enable secret: **itsasecret**

Password Line Console 0: **cisco**

Password Line vty 0 15: **cisco**

Service password-encryption

Banner motd “Acceso solo al personal autorizado”

Configuración Básica MEDELLIN2

Hostname MEDELLIN2

Enable secret: **itsasecret**

Password Line Console 0: **cisco**

Password Line vty 0 15: **cisco**

Service password-encryption

Banner motd “Acceso solo al personal autorizado”

Configuración Básica MEDELLIN3

Hostname MEDELLIN3

Enable secret: **itsasecret**

Password Line Console 0: **cisco**

Password Line vty 0 15: **cisco**

Service password-encryption

Banner motd “Acceso solo al personal autorizado”

1.1.3 CONFIGURACIÓN DEL PROTOCOLO RIP V2

Configuración RIPv2 en MEDELLIN1

Router rip

Version 2

No auto-summary

Do show ip route connected

Network 172.29.6.0

Network 172.29.6.8

Network 172.29.6.12

Passive-interface s0/0/0 (WAN A ISP).

Configuración RIPv2 en MEDELLIN2

Router rip

Version 2

No auto-summary

Do show ip route connected

Network 172.29.4.0

Network 172.29.6.0

Network 172.29.6.4

Passive-interface g0/0

Configuración RIPv2 en MEDELLIN3

Router rip

Version 2

No auto-summary

Do show ip route connected

Network 172.29.4.128

Network 172.29.6.4

Network 172.29.6.8

Network 172.29.6.12

Passive-interface g0/0

Configuración RIPv2 en BOGOTA1

Router rip

Version 2

No auto-summary

Do show ip route connected

Network 172.29.3.0

Network 172.29.3.4

Network 172.29.3.8

Passive-interface s0/0/0

Configuración RIPv2 en BOGOTA2

Router rip

Version 2

No auto-summary

Do show ip route connected

Network 172.29.1.0

Network 172.29.3.8

Network 172.29.3.12

Passive-interface g0/0

Configuración RIPv2 en BOGOTA3

Router rip

Version 2

No auto-summary

Do show ip route connected

Network 172.29.0.0

Network 172.29.3.0

Network 172.29.3.4

Network 172.29.3.12

Passive-interface g0/0

1.1.4 CONFIGURACIÓN DE RUTAS ESTÁTICAS

Configuración Rutas Estáticas de MEDELLIN1 a ISP

Configure terminal

Ip route 0.0.0.0 0.0.0.0 209.17.220.1

Configuración Rutas Estáticas de BOGOTA1 a ISP

Configure terminal

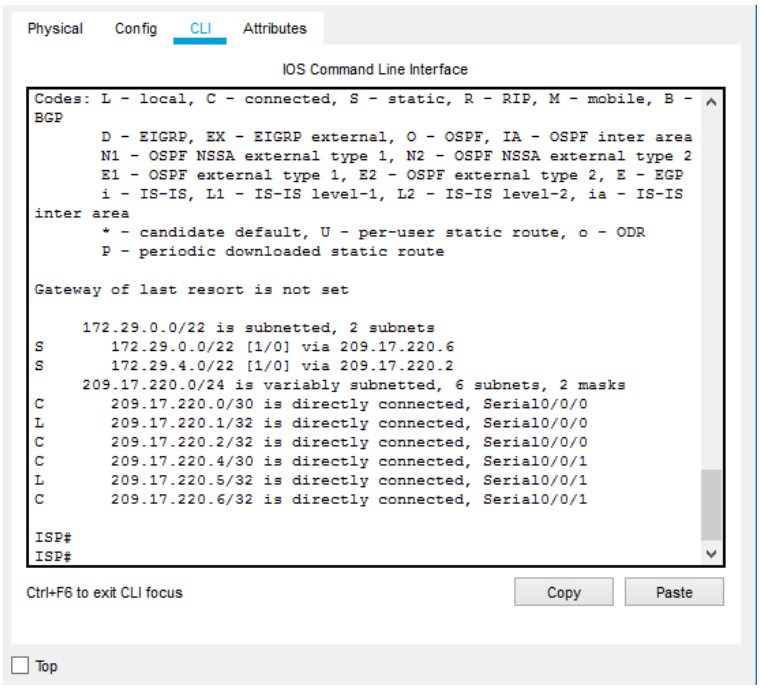
Ip route 0.0.0.0 0.0.0.0 209.17.220.5

Configuración Rutas Estáticas de ISP

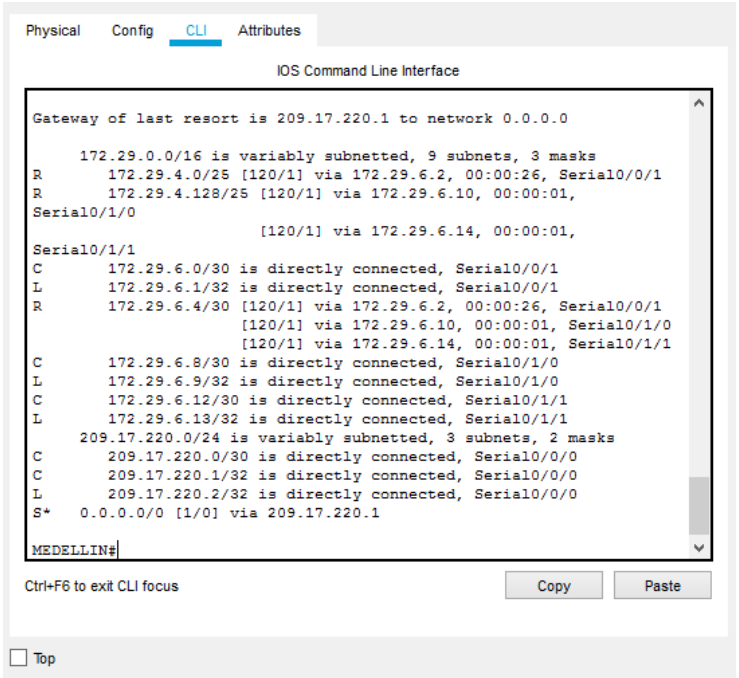
Ip route 172.29.4.0 255.255.252.0 209.17.220.2

Ip route 172.29.0.0 255.255.252.0 209.17.220.6

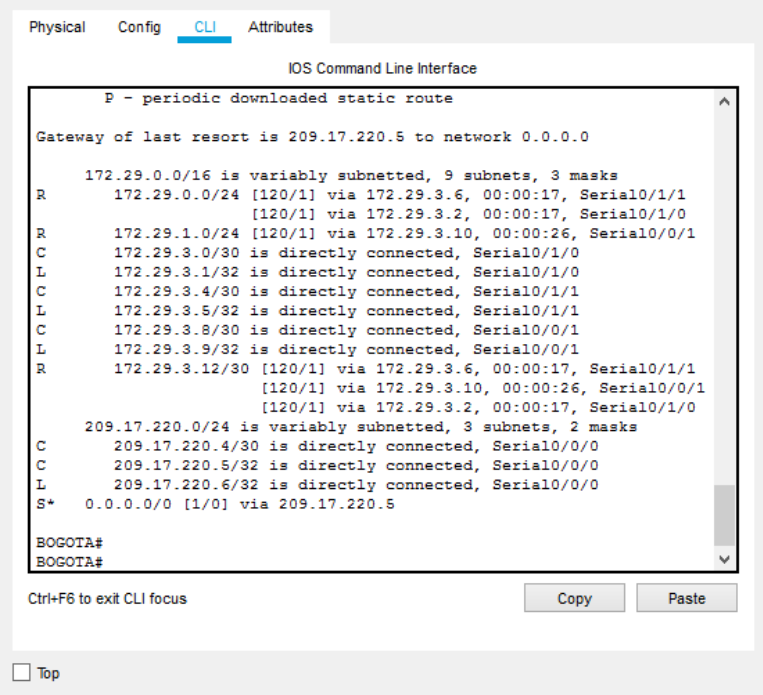
Rutas conectadas directamente a ISP



Rutas conectadas directamente a MEDELLIN1

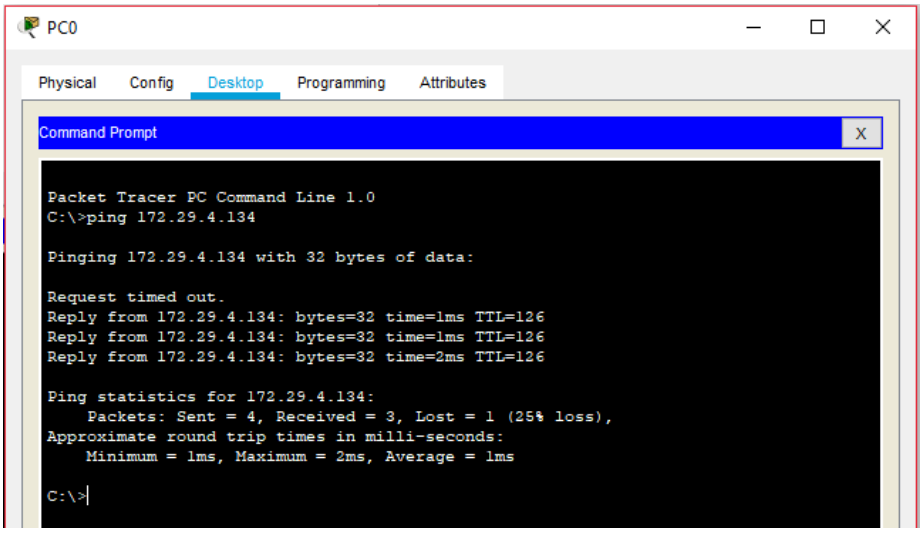


Rutas conectadas directamente a BOGOTA1

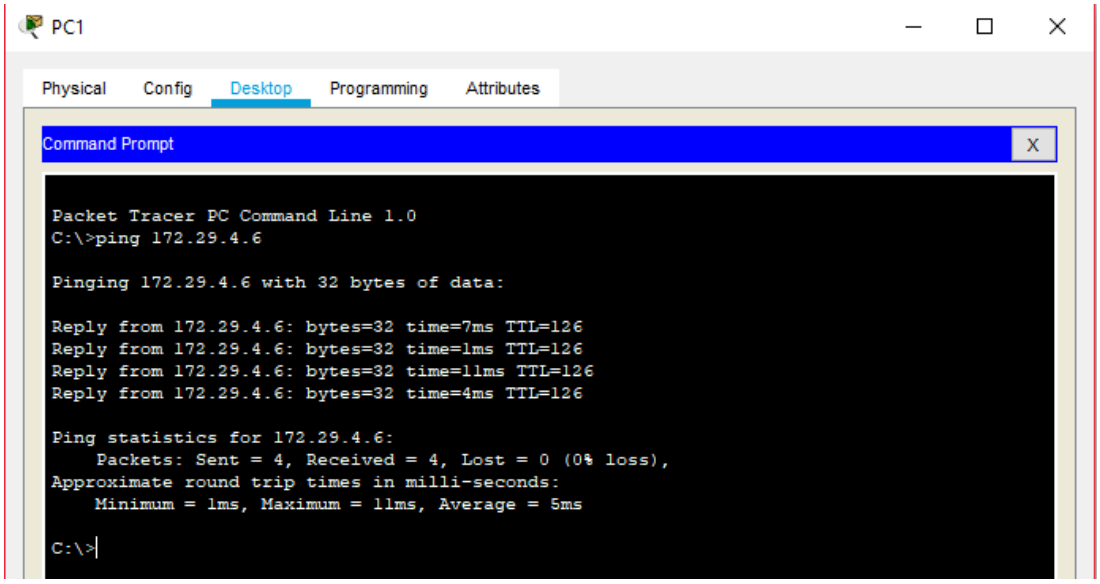


1.1.5 PRUEBAS DE CONECTIVIDAD

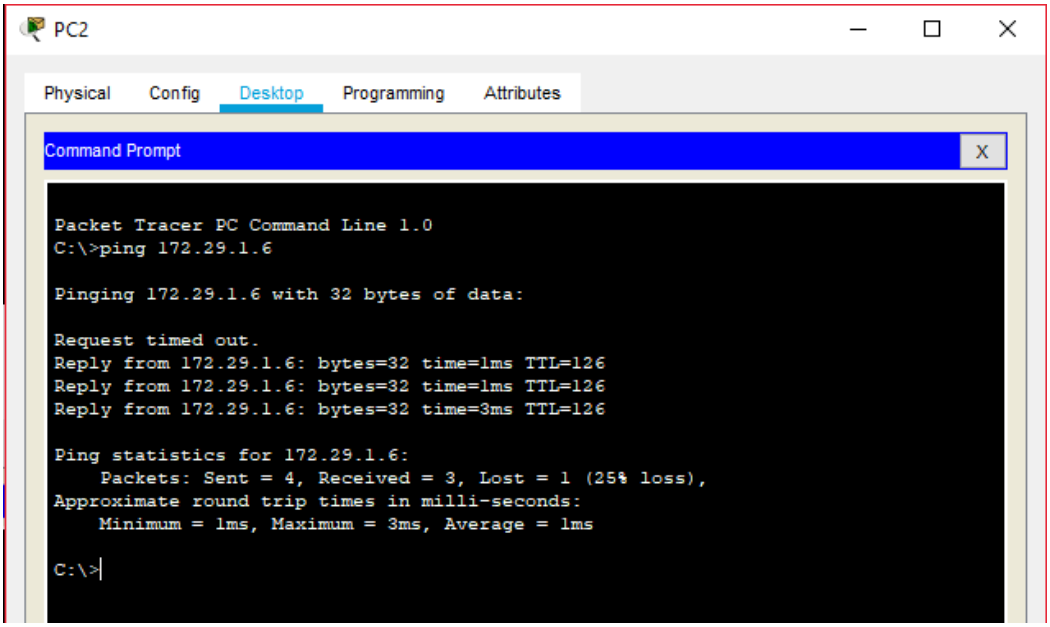
Hacer ping de PC0 a PC1



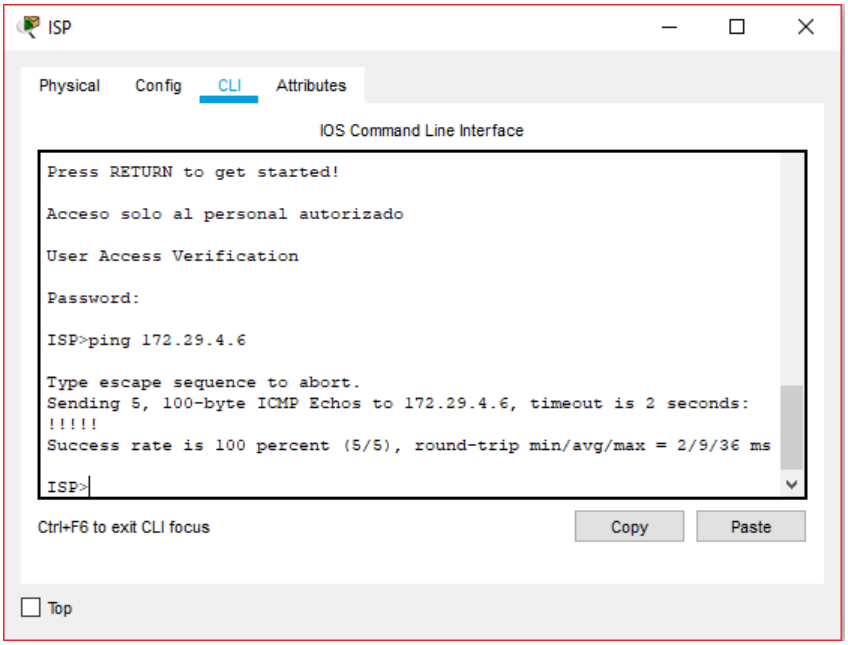
Hacer ping de PC1 a PC0



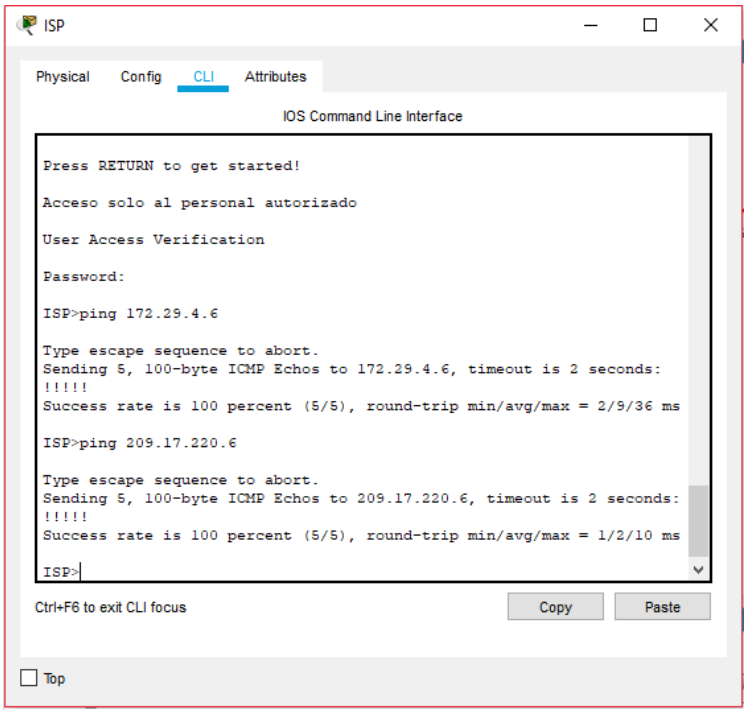
Hacer ping de PC2 a PC3



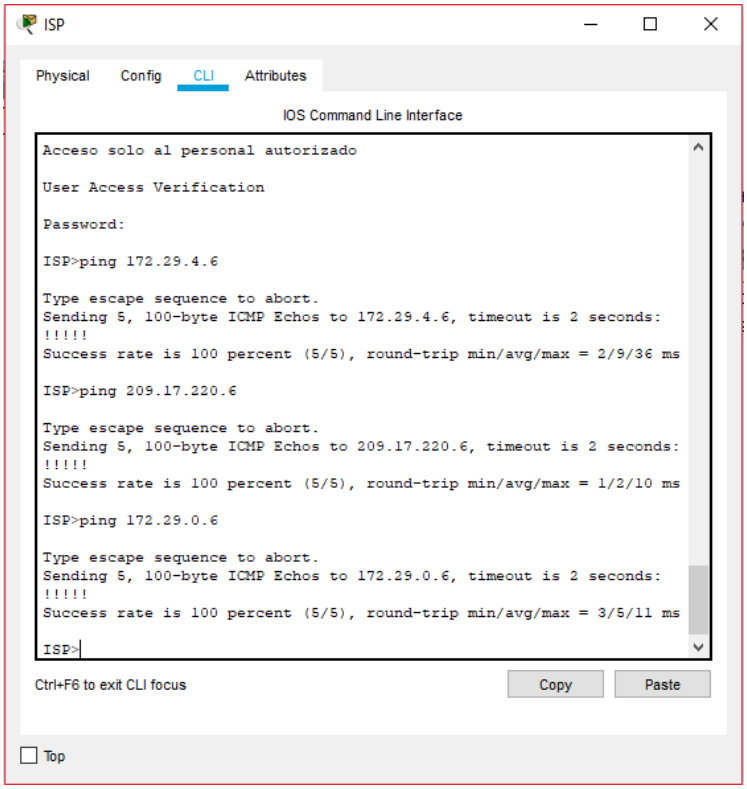
Hacer ping de ISP a PC0



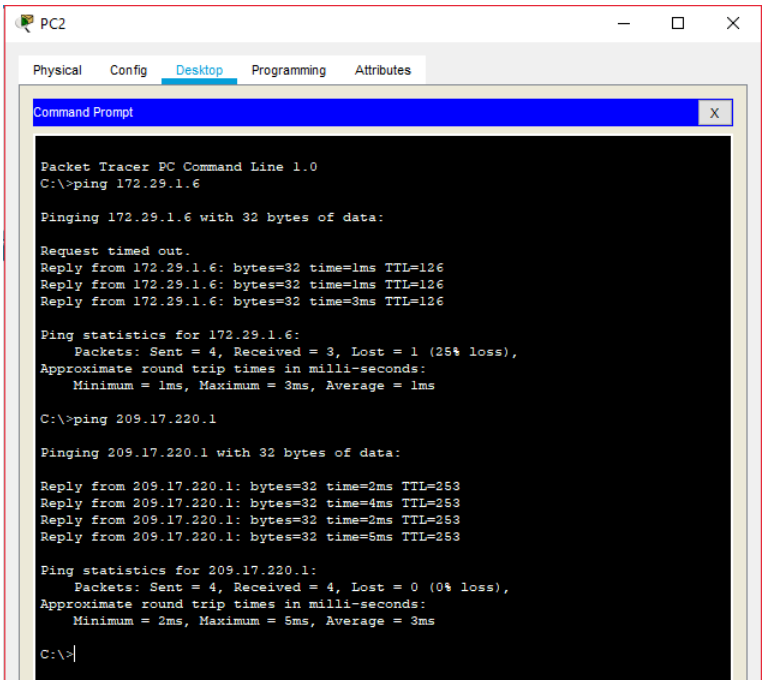
Hacer ping de ISP a BOGOTA1



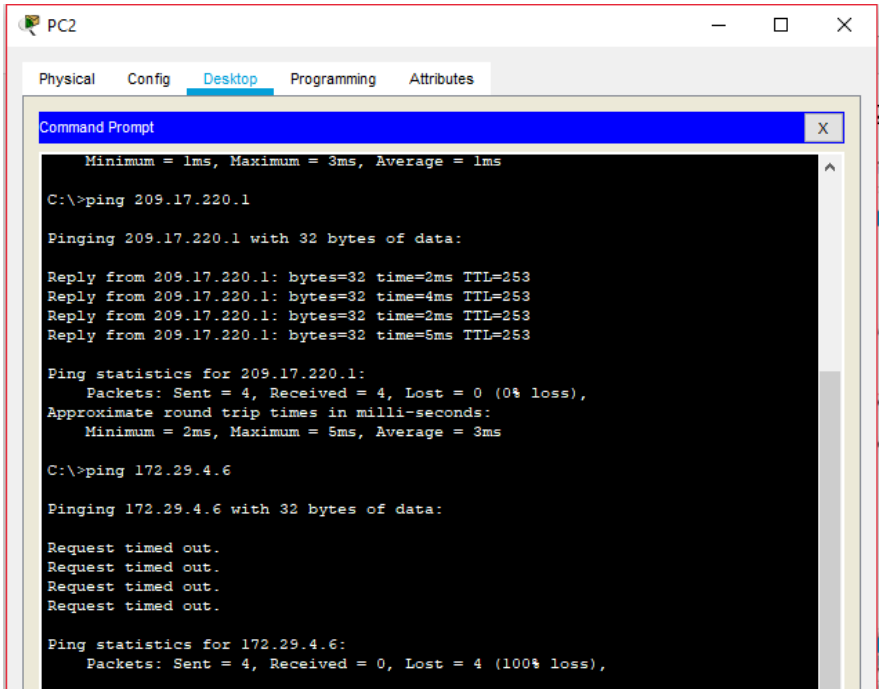
Hacer ping de ISP a PC2



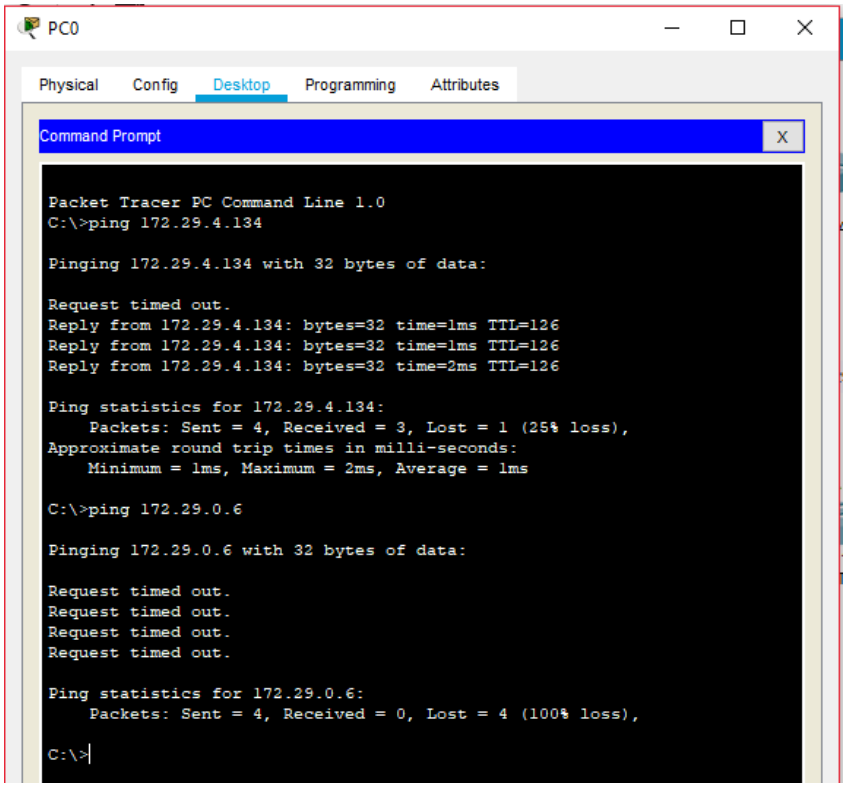
Hacer ping de PC2 a ISP



Hacer ping de PC2 a PC0

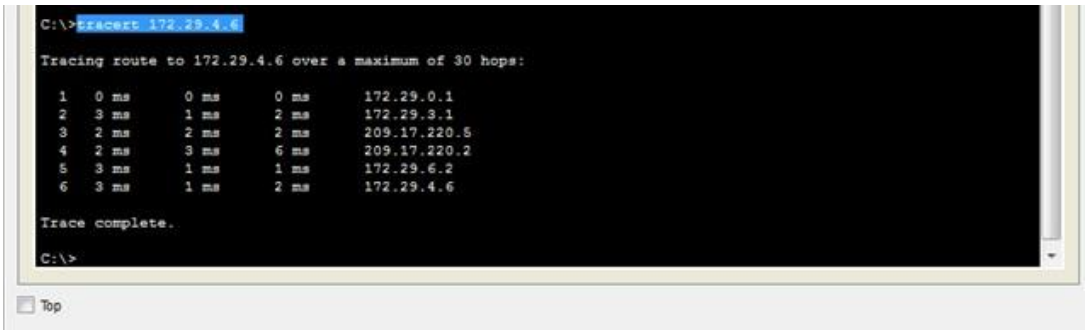


Hacer ping de PC0 a PC2

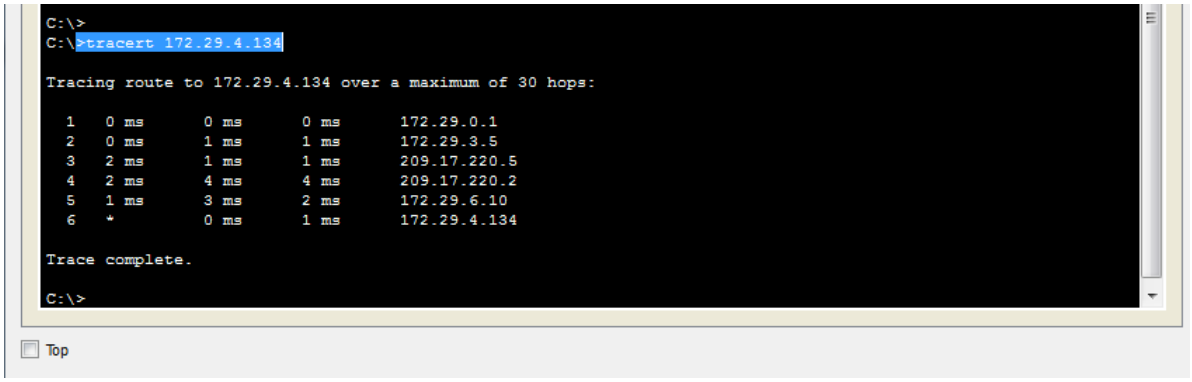


1.1.6 PRUEBAS EXTREMO A EXTREMO CON TRACERT ROUTE.

Tracert route de PC2 a PC0



Tracert route de PC2 a PC1.



1.1.7 CONFIGURACIÓN DE AUTENTICACIÓN PAP

Configuración Básica ISP

Hostname ISP

Configuración Básica MEDELLIN1

Hostname MEDELLIN

Configuración Básica BOGOTA1

Hostname BOGOTA

Autenticación PPP PAP EN ISP

Username MEDELLIN password cisco

Interface s0/0/0

Encapsulation ppp

Ppp authentication pap

Ppp pap sent-username ISP password cisco

Autenticación PPP PAP EN MEDELLIN1

Username ISP password cisco

Interface s0/0/0

Encapsulation ppp

Ppp authentication pap

Ppp pap sent-username MEDELLIN password cisco

1.1.8 CONFIGURACIÓN DE AUTENTICACIÓN CHAP

Autenticación PPP CHAP EN ISP

Username BOGOTA password cisco

Interface s0/0/1

Encapsulation ppp

Ppp authentication chap

Autenticación PPP CHAP EN BOGOTA1

Username ISP password cisco

Interface s0/0/0

Encapsulation ppp

Ppp authentication chap

1.1.9 CONFIGURACIÓN DHCP

Configuración DHCP EN MEDELLIN2

Ip dhcp excluded-address 172.29.4.1 172.29.4.5

Ip dhcp excluded-address 172.29.4.129 172.29.4.133

Ip dhcp pool MED2

Network 172.29.4.0 255.255.255.128

Default-router 172.29.4.1

Dns-server 8.8.8.8

Ip dhcp pool MED3

Network 172.29.4.128 255.255.255.128

Default-router 172.29.4.129

Dns-server 8.8.8.8

Configuración DHCP EN MEDELLIN3

Configure terminal

Interface g0/0

Ip helper-address 172.29.6.5

Configuración DHCP EN BOGOTA2

Ip dhcp excluded-address 172.29.1.1 172.29.1.5

Ip dhcp excluded-address 172.29.0.1 172.29.0.5

Ip dhcp pool BOG2

Network 172.29.1.0 255.255.255.0

Default-router 172.29.1.1

Dns-server 8.8.8.8

Ip dhcp pool BOG3

Network 172.29.0.0 255.255.255.0

Default-router 172.29.0.1

Dns-server 8.8.8.8

Configuración DHCP EN BOGOTA3

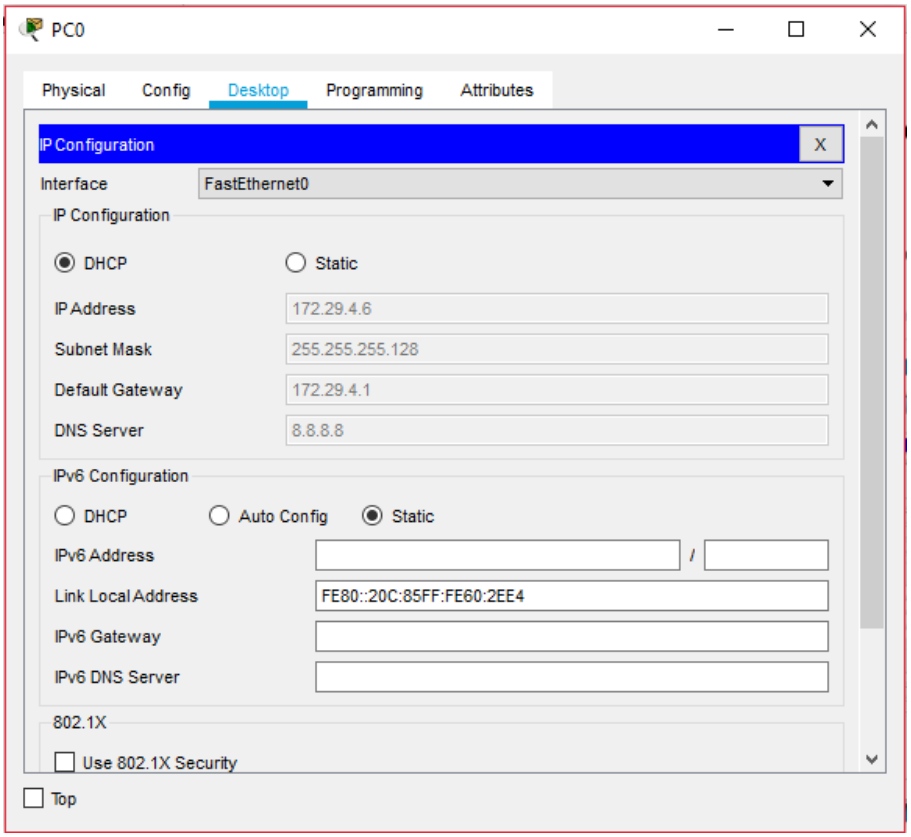
Configure terminal

Interface g0/0

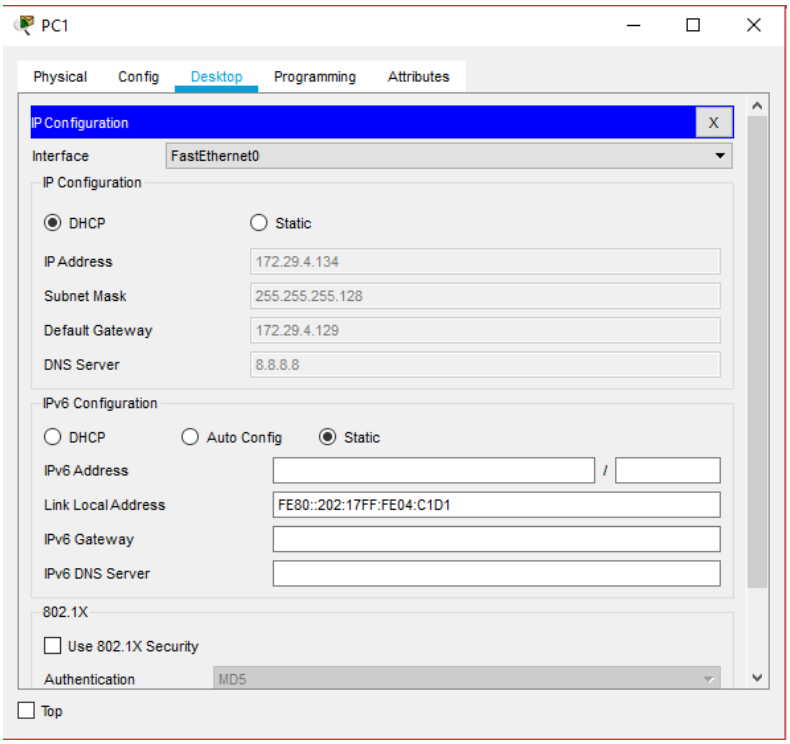
Ip helper-address 172.29.3.13

1.1.10 VERIFICACIÓN DEL SERVICIO DHCP EN FUNCIONAMIENTO EN AMBOS EXTREMOS.

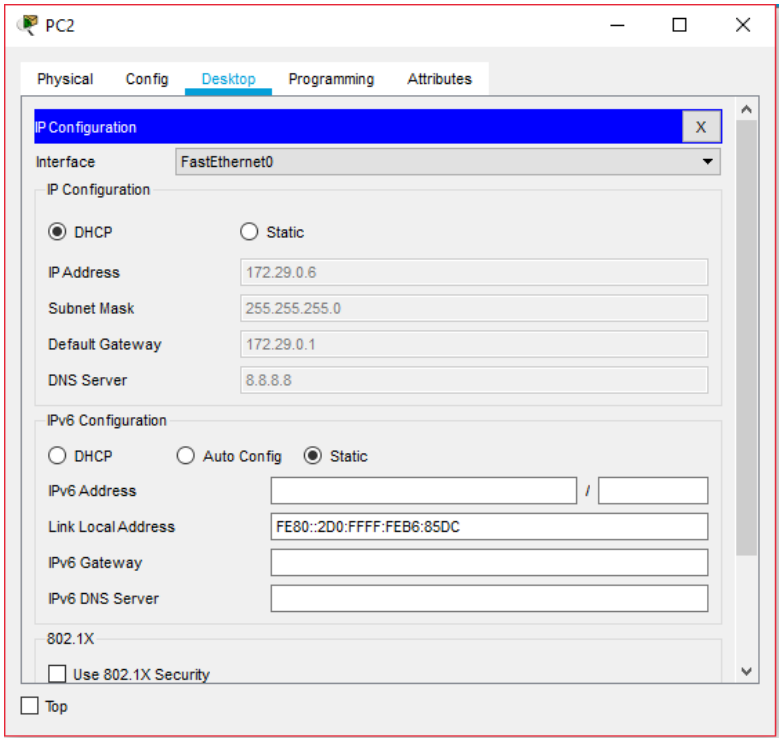
Verificación del servicio DHCP en funcionamiento en PC0



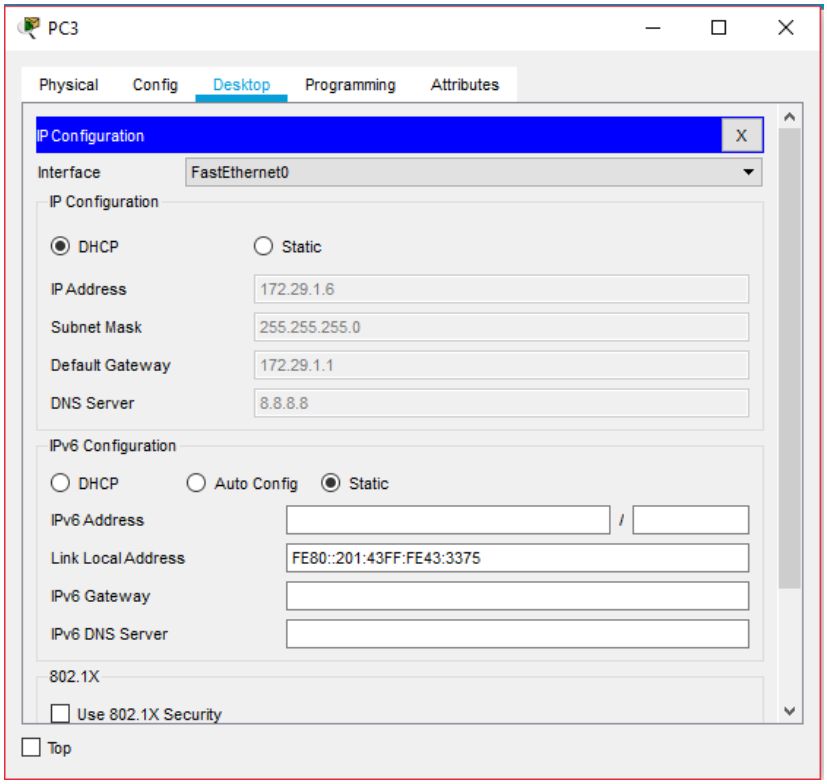
Verificación del servicio DHCP en funcionamiento en PC1



Verificación del servicio DHCP en funcionamiento en PC2



Verificación del servicio DHCP en funcionamiento en PC3



1.1.11 CONFIGURACIÓN DE NAT

NAT en MEDELLIN1

Configure terminal

Ip nat inside source list 1 interface s0/0/0 overload

Access-list 1 permit 172.29.4.0 0.0.3.255

Int s0/0/0

Ip nat outside

Int s0/01

Ip nat inside

Int s0/1/0

Ip nat inside

Int s0/1/1

Ip nat inside

NAT en BOGOTA1

Configure terminal

Ip nat inside source list 1 interface s0/0/0 overload

Access-list 1 permit 172.29.0.0 0.0.3.255

Int s0/0/0

Ip nat outside

Int s0/0/1

Ip nat inside

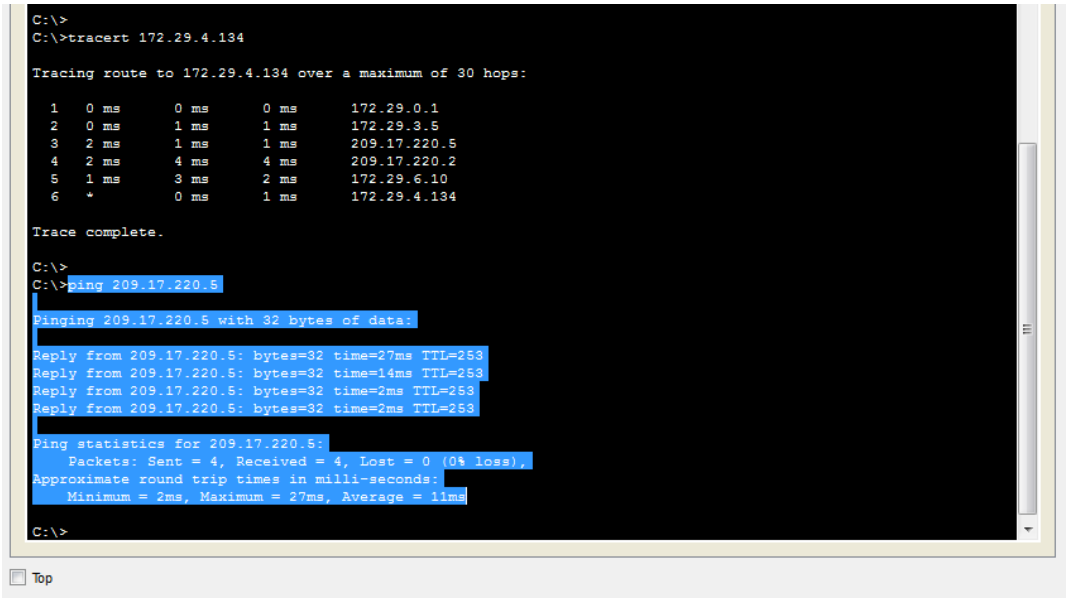
Int s0/1/0

Ip nat inside

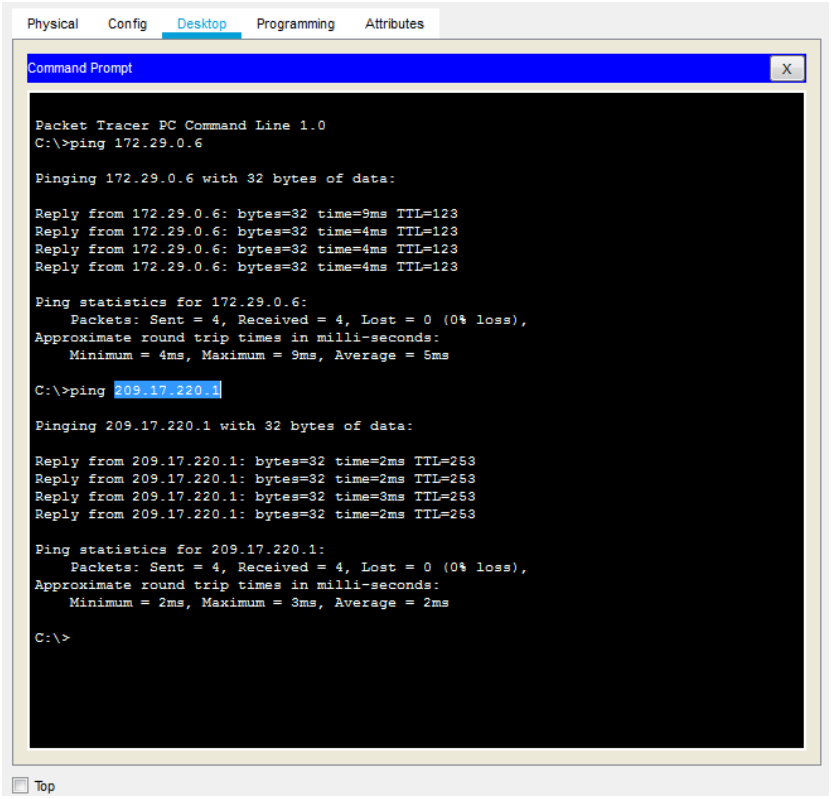
Int s0/1/1

Ip nat inside

Ping pc2 a ISP

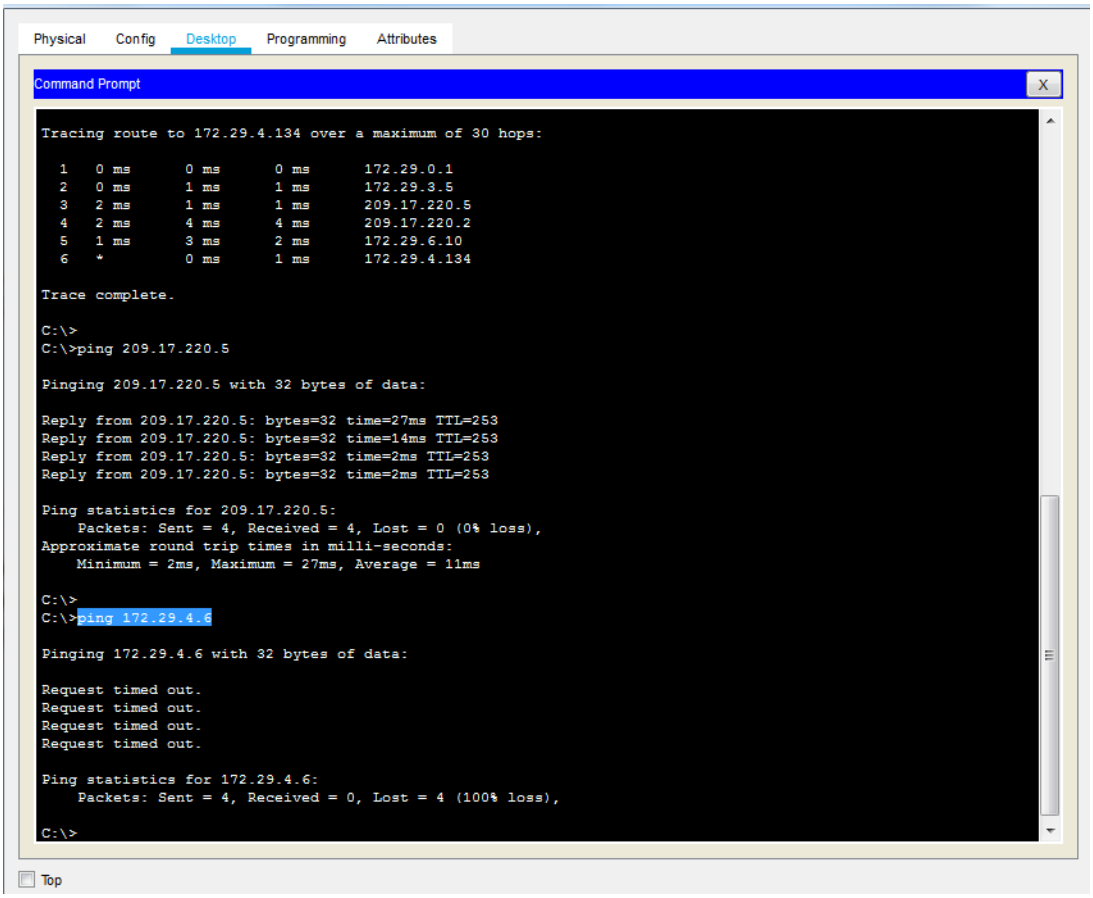


Ping PC0 a ISP



Ping es satisfactorio

Ping de PC2 a PC0



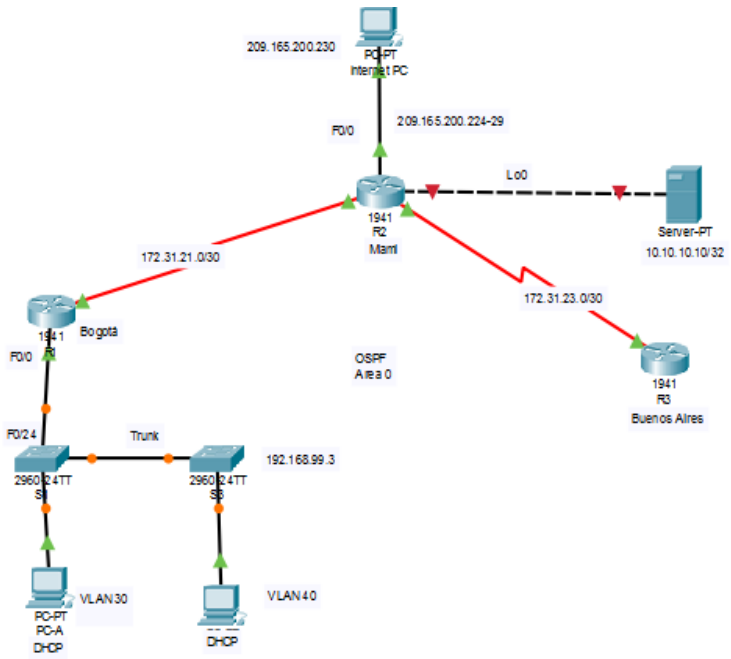
Ping no es satisfactorio porque NAT lo bloquea.

2.0 DESCRIPCIÓN DEL ESCENARIO 2

Una empresa de Tecnología posee tres sucursales distribuidas en las ciudades de Miami, Bogotá y Buenos Aires, en donde el estudiante será el administrador de la red, el cual deberá configurar e interconectar entre sí cada uno de los dispositivos que forman parte del escenario, acorde con los lineamientos establecidos para el direccionamiento IP, protocolos de enrutamiento y demás aspectos que forman parte de la topología de red.

2.1 SOLUCION DEL ESCENARIO 2

2.1.1 Topología



Dispositivo	Interface	Direccion IP	Masdca de Subred	Puerta de enlace predeterminada
R1	G0/0	192.168.99.1	255.255.255.0	
	S0/0/0	172.31.21.1	255.255.255.252	
R2	S0/1/0	172.31.21.2	255.255.255.252	
	S0/1/1	172.31.23.1	255.255.255.252	
	G0/1	10.10.10.10	255.255.255.255	
R3	S0/1/0	172.32.23.2	255.255.255.252	
	Lo4	192.168.4.1	255.255.255.255	
	Lo5	192.168.5.1	255.255.255.255	
	Lo6	192.168.6.1	255.255.255.255	
PC-A	NIC	DHCP	DCHP	DHCP
PC-B	NIC	DHCP	DHCP	DHC
PC Internet	NIC	209.165.200.230	255.255.255.248	209.168.200.225

2.1.2 CONFIGURACIÓN BÁSICA ROUTER R1.

Enable

Configure terminal

Hostname R1

Enable secret: cisco

Service password-encryption

Banner motd “Acceso solo al personal autorizado”

Password Línea de consola: cisco

Password Líneas VTY: cisco

Configuración del direccionamiento para Router R1.

Interface s0/0/0

Description Bogota

Ip address 172.31.21.0/30

Clock rate 128000

No shutdown

Interface F0/0

Interface F0/0

Ip address 192.168.99.1 (esta red habilitará la LAN).

No shutdown

2.1.3 CONFIGURACIÓN BÁSICA ROUTER R2.

Enable

Configure terminal

Hostname R2

Enable secret: cisco

Service password-encryption

Banner motd “Acceso solo al personal autorizado”

Password Línea de consola: cisco

Password Líneas VTY: cisco

Configuración del direccionamiento para Router R2.

Interface fa0/0 (interface g0/0 – Internet).

Description Internet

Ip address 209.165.200.225 255.255.255.248

Dúplex auto

Speed auto

No shutdown

Interface Lo0 (WEB SERVER).

Configure terminal

Interface loopback 0

Ip address 10.10.10.10 255.255.255.255

Description conexión a Web Server.

No shutdown.

Interface s0/0/0.

Interface s0/0/0.

Ip address 172.31.23.2 255.255.255.252

Clock rate 128000

No shutdown.

Interface s0/0/1.

Interface s0/0/1.

Ip address 172.31.21.2 255.255.255.252

No shutdown

2.1.4 CONFIGURACIÓN BÁSICA ROUTER R3.

Enable

Configure terminal

Hostname R3

Enable secret: cisco

Service password-encryption

Banner motd “Acceso solo al personal autorizado”

Password Línea de consola: cisco

Password Líneas VTY: cisco

Configuración del direccionamiento para Router R3.

Interface s0/0/1

Interface s0/0/1

Ip address 172.31.23.1 255.255.255.252

Interface loopback4

Ip address 192.168.4.1 255.255.255.0

Exit

Interface loopback5

Ip address 192.168.5.1 255.255.255.0

Exit.

Interface loopback6

Ip address 192.168.6.1 255.255.255.0

Exit

2.1.5 CONFIGURACIÓN BÁSICA SWITCH S1.

Enable

Configure terminal

Hostname S1

Enable secret: cisco

Service password-encryption

Banner motd “Acceso solo al personal autorizado”

Password Línea de consola: cisco

Password Líneas VTY: cisco

2.1.6 CONFIGURACIÓN BÁSICA SWITCH S3.

Enable

Configure terminal

Hostname S3

Enable secret: cisco

Service password-encryption

Banner motd “Acceso solo al personal autorizado”

Password Línea de consola: cisco

Password Líneas VTY: cisco

2.1.7 CONFIGURACIÓN DEL PROTOCOLO DE ENRUTAMIENTO OSPFV2

Router R1

Configure terminal

Router ospf 2

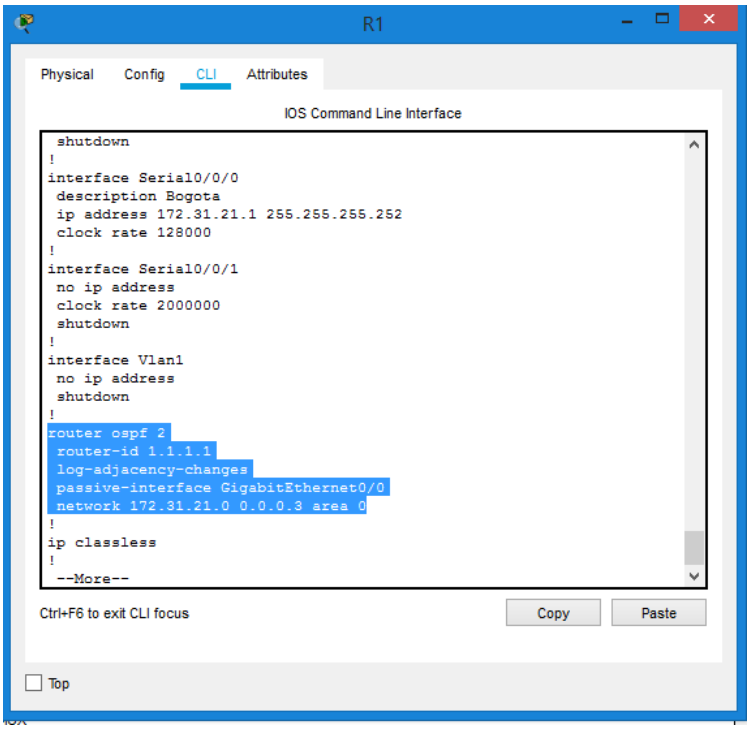
Network 172.31.21.0 0.0.0.3 area 0

Router-id 1.1.1.1 – **luego se recarga el dispositivo para que los cambios surjan efectos.**

Configure terminal

Router ospf 2

Passive-interface g0/0



Evidencia del funcionamiento del protocol ospf 2

Configuración pasiva de la LAN

Router ospf 2

Passive-interface g0/0

Passive-interface g0/1

Ancho de banda de enlace serial de 256 Kb/S

Interface s0/0/0

Bandwidth 256

Interface s0/0/1

Bandwidth 256

Costo de la métrica

int s0/0/0

ip ospf cost 9500

Router R2

Configure terminal

Router ospf2

Network 172.31.23.0 0.0.0.255 area 0

Network 172.31.21.0 0.0.0.255 area 0

Router-id 5.5.5.5

Configuración pasiva de la LAN

Router ospf 2

Passive-interface g0/0

Passive-interface g0/1

Ancho de banda de enlace serial de 256 Kb/S

Interface s0/0/0

Bandwidth 256

Interface s0/0/1

Bandwidth 256

Costo de la métrica

Interface s0/0/0

Ip ospf cost 9500

Router R3

Configure terminal

Router ospf2

Network 192.31.23.0 0.0.0.3 area 0

Router-id 8.8.8.8

Configuración pasiva de la LAN

Router ospf 2

Passive-interface g0/0

Passive-interface g0/1

Ancho de banda de enlace serial de 256 Kb/S

Interface s0/0/0

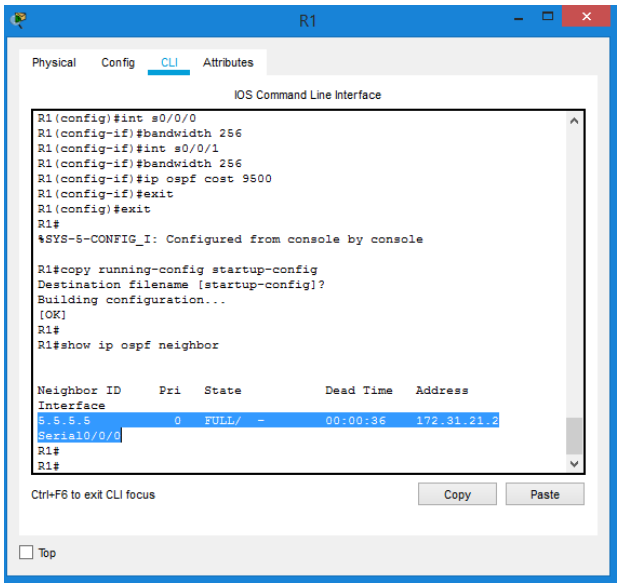
Bandwidth 256

Interface s0/0/1

Bandwidth 256

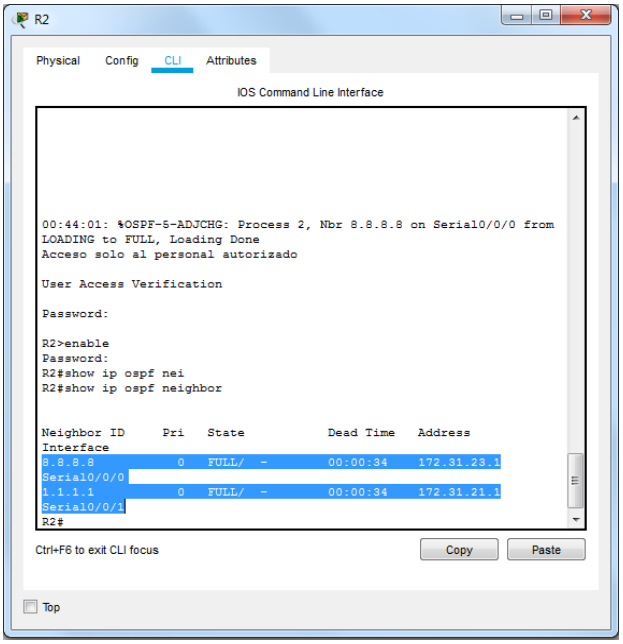
2.1.8 VISUALIZACIÓN DE TABLAS DE ENRUTAMIENTO Y ROUTERS CONECTADOS POR OSPFV2

En R1



Aparece la interfaz 5.5.5.5 correspondiente al R2.

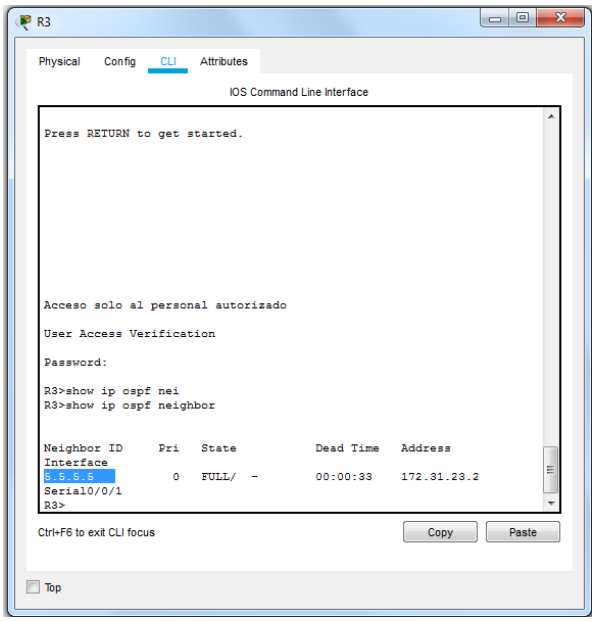
En R2.



Muestra la interfaz 8.8.8.8 correspondiente al R3.

Muestra la interfaz 1.1.1.1 correspondiente al R1.

En R3.

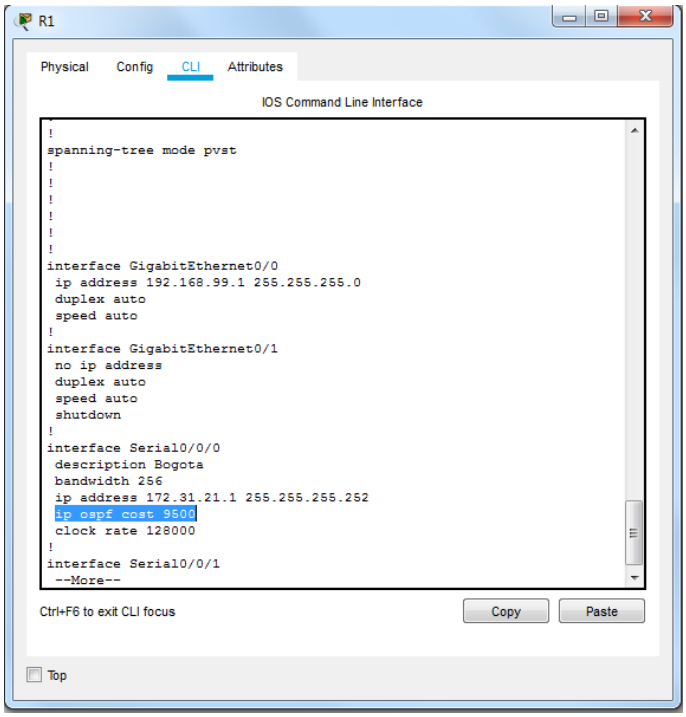


Muestra la interfaz 5.5.5.5 correspondiente al R2.

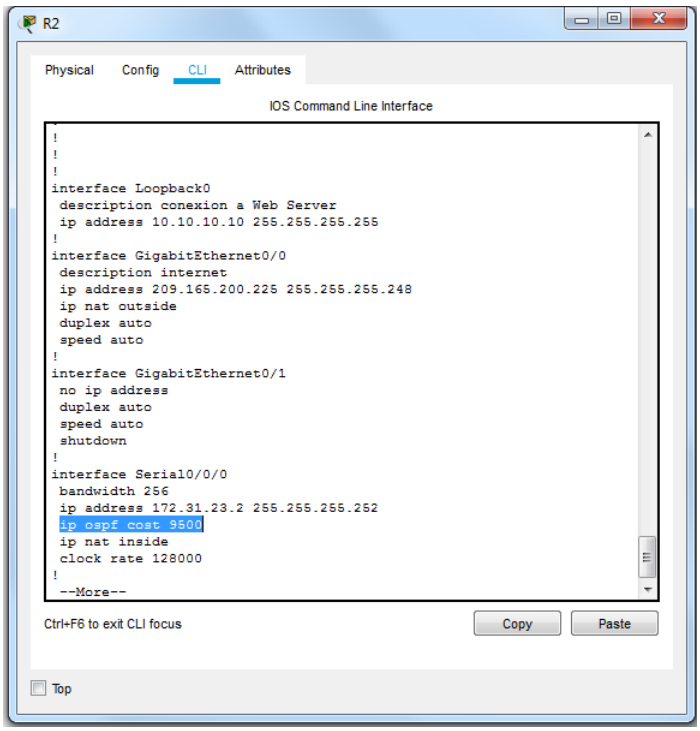
2.1.9 VISUALIZAR LISTA RESUMIDA DE INTERFACES POR OSPF EN DONDE SE ILUSTRE EL COSTO DE CADA INTERFAZ

El costo de las métricas fue aplicado a las interfaces s0/0/0 de cada router, como lo solicita la guía.

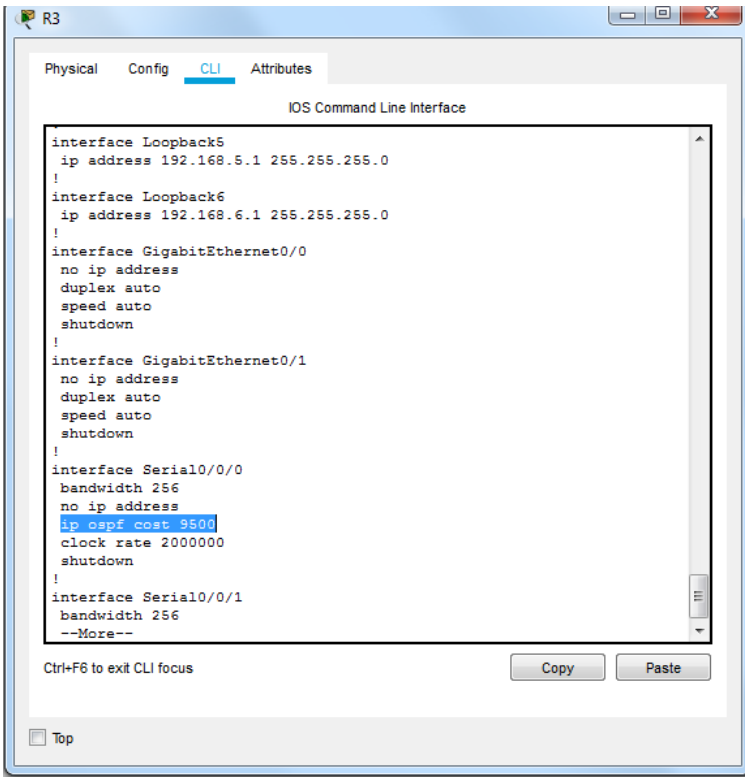
En R1.


R1
Physical
Config
CLI
Attributes
IOS Command Line Interface
!
spanning-tree mode pvst
!
!
!
!
!
!
interface GigabitEthernet0/0
 ip address 192.168.99.1 255.255.255.0
 duplex auto
 speed auto
!
interface GigabitEthernet0/1
 no ip address
 duplex auto
 speed auto
 shutdown
!
interface Serial0/0/0
 description Bogota
 bandwidth 256
 ip address 172.31.21.1 255.255.255.252
 ip ospf cost 9500
 clock rate 128000
!
interface Serial0/0/1
 --More--
Ctrl+F6 to exit CLI focus
Copy
Paste
Top

En R2.

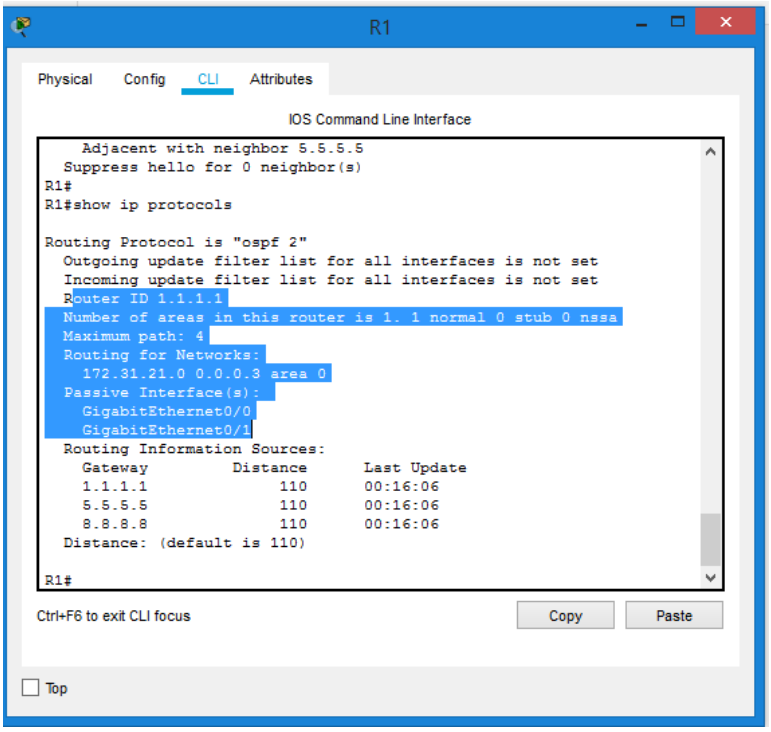

R2
Physical
Config
CLI
Attributes
IOS Command Line Interface
!
!
!
interface Loopback0
 description conexion a Web Server
 ip address 10.10.10.10 255.255.255.255
!
interface GigabitEthernet0/0
 description internet
 ip address 209.165.200.225 255.255.255.248
 ip nat outside
 duplex auto
 speed auto
!
interface GigabitEthernet0/1
 no ip address
 duplex auto
 speed auto
 shutdown
!
interface Serial0/0/0
 bandwidth 256
 ip address 172.31.23.2 255.255.255.252
 ip ospf cost 9500
 ip nat inside
 clock rate 128000
!
 --More--
Ctrl+F6 to exit CLI focus
Copy
Paste
Top

En R3.

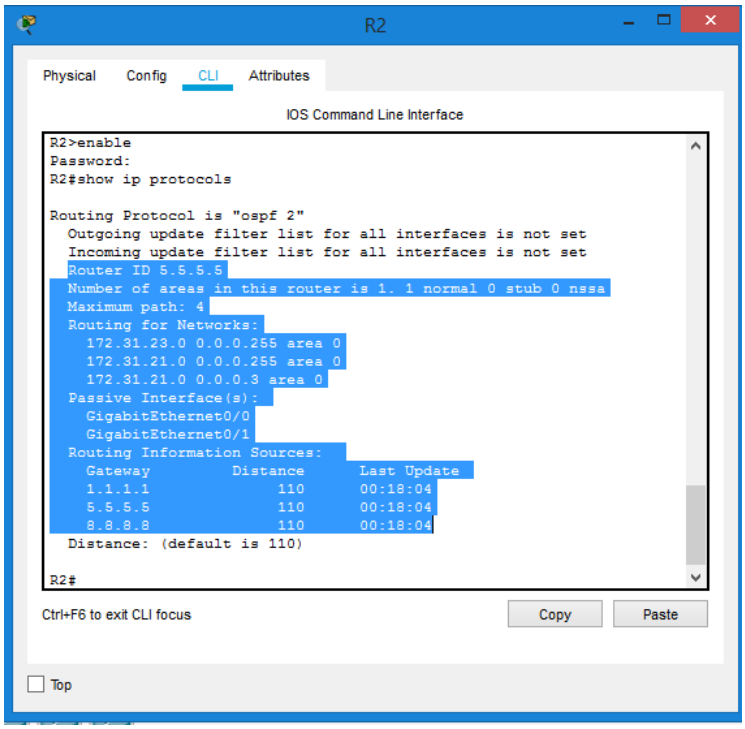


2.1.10 VISUALIZAR EL OSPF PROCESS ID, ROUTER ID, ADDRESS SUMMARIZATIONS, ROUTING NETWORKS, AND PASSIVE INTERFACES CONFIGURADAS EN CADA ROUTER.

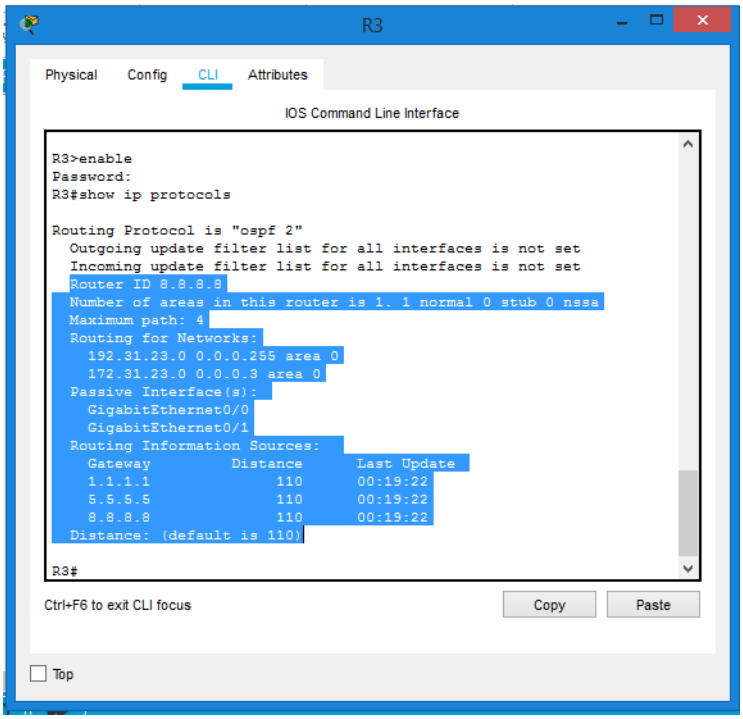
En R1. (show ip protocols).



En R2. (show ip protocols).



En R3. (show ip protocols).



2.1.11 CONFIGURACIÓN DE PUERTOS TRONCALES

S3: En el puerto fa 0/3 del S3, estableciendo un enlace troncal con el Switch S2.

Interface fa 0/3

Sw mo tr

S1: En el puerto fa 0/3 del S1, estableciendo un enlace troncal con el Switch S3.

Interface fa 0/3

Sw mo tr

2.1.12 CONFIGURACIÓN DE VLANS

Vlan 30 en S1

Configure terminal

Vlan 30

Name Administracion

Exit

Interface fa 0/1

Sw acc vlan 30

Vlan 40 en S3

Configure terminal

Vlan 40

Name mercadeo

Exit

Int fa 0/1

Sw acc vlan 40

2.1.13 SEGURIDAD EN LOS SWITCHES

S1.

Interface fa 0/1

Switchport mode Access

Switchport port-security

Switchport port-security máximum 1

Switchport port-security violation shutdown

Switchport port-security mac-address sticky

Interface fa 0/3

Switchport mode Access

Switchport port-security

Switchport port-security máximum 1

Switchport port-security violation shutdown

Switchport port-security mac-address sticky

Interface fa 0/24

Switchport mode Access

Switchport port-security

Switchport port-security máximum 1

Switchport port-security violation shutdown

Switchport port-security mac-address sticky

S3.

Interface fa 0/1

Switchport mode Access

Switchport port-security

Switchport port-security máximum 1

Switchport port-security violation shutdown

Switchport port-security mac-address sticky

Interface fa 0/3

Switchport mode Access

Switchport port-security

Switchport port-security máximum 1

Switchport port-security violation shutdown

Switchport port-security mac-address sticky

2.1.14 DESHABILITACIÓN DNS LOOKUP EN SWITCH3

Config t

No ip domain-lookup

2.1.15 ASIGNAR DIRECCIONES IP A LOS SWITCHES ACORDE A LOS LINEAMIENTOS

S1

Interface vlan 99

Ip address 192.168.99.2 255.255.255.0

S3

Interface vlan 99

Ip address 192.168.99.3 255.255.255.0

2.1.16 DESACTIVAR TODAS LAS INTERFACES QUE NO SEAN UTILIZADAS EN EL ESQUEMA DE RED

S3.

Interface ra fa 0/2

Sh

Interface ra fa 04/-24

Sh

S1.

Interface f0/2

Sh

Interface ra fa 04/-23

Sh

2.1.17 CONFIGURAR R1 COMO SERVIDOR DHCP PARA LAS VLANS 30 Y 40

Ip dhcp excluded-address 192.168.30.1

Ip dhcp excluded-address 192.168.40.1

Ip dhcp pool Administracion

Network 192.168.30.0 255.255.255.0

default-router 192.168.30.1 255.255.255.0

dns-server 10.10.10.11

Ip dhcp pool Mercadeo

Network 192.168.40.0 255.255.255.0

default-router 192.168.40.1 255.255.255.0

dns-server 10.10.10.11

ip domain-name ccna-unad.com

CONCLUSIÓN

Con el desarrollo del presente trabajo pudimos demostrar las destrezas y conocimiento adquiridos a lo largo del curso en cuanto a configuración de equipos de red Cisco, como Routers, Switches y aplicar comandos, así como también conceptualizar con claridad el termino de red, que no es más que un conjunto de equipos (computadoras y/o dispositivos) conectados por medio de cables, señales, ondas o cualquier otro método de transporte de datos, que comparten información (archivos), recursos (CD-ROM, impresoras, etc.) y servicios (acceso a internet, e-mail, chat), etc.

BIBLIOGRAFÍA

Configuración Troncal 802.1q. (S.F.).

Https://Www.Cisco.Com/C/Es_Mx/Support/Docs/Switches/Catalyst-4000-Series-Switches/24064-171.Html

Ariganello, E., & Sevilla, B. (2011). Redes CISCO - guía de estudio para la certificación CCNP (No. 004.6 A73).

Benchimol, D. (2010). Redes Cisco-Instalacion y administracion de hardware y software.

CISCO. (s.f.). Principios básicos de routing y switching: Listas de Control de Acceso. (2017), Tomado de: https://static-courseassets.s3.amazonaws.com/RSE503/es/index.html#9.0.1

Principios básicos de routing y switching: Traducción de direcciones de red para IPv4. (2017), Tomado de: https://static-courseassets.s3.amazonaws.com/RSE503/es/index.html#11.0

DHCP. Principios de Enrutamiento y Conmutación. (2014) Recuperado de: https://static-course-assets.s3.amazonaws.com/RSE50ES/module10/index.html#10.0.1.1

Teare, D., Vachon B., Graziani, R. (2015). CISCO Press (Ed). Implementing IPv4 in the Enterprise Network. Implementing Cisco IP Routing (ROUTE) Foundation Learning Guide CCNP ROUTE 300-101. Recuperado de https://1drv.ms/b/s!AmIJYei-NT1IlnMfy2rhPZHwEoWx

Segui, F. B. (2015). Configuración DHCP en routers CISCO.